**IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF ILLINOIS EASTERN DIVISION**

| | |
|---|---|
| ALEX PRELIPCEANU, individually and on behalf of similarly situated individuals,<br><br>Plaintiff,<br><br>v.<br><br>JUMIO CORPORATION, a Delaware Corporation,<br><br>Defendant. | Case No. 1:19-cv-00561<br><br>Honorable Robert W. Gettleman |

**JUMIO CORPORATION'S MEMORANDUM OF LAW IN SUPPORT OF ITS MOTION TO DISMISS PLAINTIFF'S COMPLAINT**

# TABLE OF CONTENTS

## TABLE OF AUTHORITIES

**Page(s)**

**CASES**

**TABLE OF AUTHORITIES**
**(continued)**

**Page(s)**

**TABLE OF AUTHORITIES**
**(continued)**

**Page(s)**



**STATUTES**



**RULES**

## I. INTRODUCTION

This lawsuit is one of over 170 similar cases filed in the last four years alleging violations of the Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1, *et seq*. ("BIPA"), which regulates the collection, storage, and disclosure of biometric identifiers and biometric information ("Biometric Data")[1] and provides for substantial "liquidated" damages for certain violations.

Defendant Jumio Corporation ("Jumio") offers its software product, "Netverify," to customers like banks, airlines, educational institutions, and retailers that sell products and services over the Internet (Jumio's "Customers"). *See* Complaint, Dkt. 1, Ex. 1 ("Compl.") ¶ 19. Netverify, operating within a Customer's website, uses facial recognition technology to enable the Customer to confirm the ages and identities of its end users. *See id.* ¶ 21.

Plaintiff Alex Prelipceanu is an Illinois resident[2] who purchased age-restricted products from a company he does not identify in the Complaint, using the company's website to make the purchase. *See id*. ¶¶ 22, 24. To ensure that Prelipceanu was who he purported to be and that he was old enough to buy the products, the company, a Jumio Customer, used Netverify to validate his age and identity. Prelipceanu now alleges that this process violated BIPA, *see* Compl. ¶ 45, and that by violating BIPA, Jumio is liable for negligence, *see id.* ¶ 57.

The Court should dismiss Prelipceanu's claims under Federal Rule of Civil Procedure 12(b)(6). First, when stripped of the allegations that merely parrot BIPA and the conclusory allegations that BIPA has been violated, the Complaint is insufficient to state a claim and the Court should dismiss Prelipceanu's claims for that reason alone. The Court should also dismiss Prelipceanu's claim that Jumio disclosed his Biometric Data in violation of BIPA § 14/15(d) because, even if such a disclosure occurred (and Prelipceanu does not allege facts that would support such a conclusion), the disclosure would fall squarely within the exceptions set out in §

[1] BIPA defines the terms "biometric identifiers" and "biometric information." Jumio refers to these collectively as "Biometric Data" in this Motion, though that term is not used in BIPA.

[2] Solely for purposes of this motion, Jumio will assume that the adequately pleaded allegations in the Complaint are true. Jumio does not concede the accuracy of any of Prelipceanu's allegations.

14/15(d). In addition, the Court should dismiss Prelipceanu's claim for violation of BIPA § 14/15(a), which asserts that Jumio lacked a retention policy for Biometric Data, because Jumio's judicially-noticeable policy is both publicly available and BIPA-compliant. Finally, Prelipceanu's negligence claim is entirely duplicative of his BIPA claim, and should be dismissed on that basis and for the independent reason that Prelipceanu does not allege facts establishing either a duty owed or cognizable damage resulting from Jumio's alleged breach.

## II. BACKGROUND

### A. BIPA: An Overview

BIPA regulates the "collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." BIPA § 14/5(g). It was enacted in 2008 to encourage the "growing" use of Biometric Data in Illinois, because biometric technology "promise[d] streamlined financial transactions and security screenings." *Id.* § 14/5(a). The first case alleging a BIPA violation was not filed until 2015, when plaintiffs sued Facebook in *Licata v. Facebook, Inc.* *See* Complaint, *Licata*, No. 2015CH05427 (Ill. Cir. Ct., Cook Cty. April 1, 2015). Since then, over 170 putative class actions asserting violations of BIPA have been filed, most of them in Illinois federal and state courts. Many of these complaints, including the Complaint in this case, follow standard formats. None of these cases has proceeded to judgment and few have progressed to the discovery phase.

### B. Jumio and Netverify

Jumio is headquartered in California and serves Customers throughout the world. *See* Jumio, About Jumio, https://www.jumio.com/about/ (last visited Mar. 29, 2019) (attached as Exhibit A).[3] Jumio's website explains that it offers its Customers "identity verification and

[3] The Court may properly consider Jumio's website without converting the motion to dismiss into a motion for summary judgment. *See Venture Assocs. Corp. v. Zenith Data Sys. Corp.*, 987 F.2d 429, 431 (7th Cir. 1993) ("Documents that a defendant attaches to a motion to dismiss are considered part of the pleadings if they are referred to in the plaintiff's complaint and are central to her claim."). Prelipceanu references Jumio's website in his Complaint and information from Jumio's website about how Netverify operates is central to his claims. *See* Compl. ¶ 20 n.1. Prelipceanu cannot cherry-pick only those portions of Jumio's website that best support his claims and bar Jumio from referencing other portions. *See Pennington v. Travelex Currency Servs., Inc.*, 114 F. Supp. 3d 697, 703 n.7 (N.D. Ill. 2015) (holding that

authentication solutions [that] leverage the power of biometrics, AI and the latest technologies to quickly verify the digital identities of new customers and existing users." Compl. ¶ 20 n.1 (citing Jumio, End-to-End AI-Powered Identity Verification & Authentication, https://www.jumio.com/trusted-identity/netverify/ (last visited Mar. 29, 2019) (attached as Exhibit B)). Jumio's Privacy Policy is publicly available on every page of Jumio's website, including the webpage Prelipceanu cited in his Complaint. *See id.*; *see also* Jumio, Jumio Corp. Privacy Policy for Online Services, https://www.jumio.com/legal-information/privacy-policy/jumio-inc-privacy-policy-for-online-services/ (last visited Mar. 29, 2019) (attached as Exhibit C) ("Jumio Privacy Policy").

Jumio's Customers include vendors that use Netverify within their own websites to verify the ages of their customers, the end users. *See* Compl. ¶ 2. To "purchase goods or services" from a Jumio Customer using Netverify, end users must upload identity documents and "a photo of themselves or otherwise undergo a scan of their facial geometry, often taken through a webcam." *Id.* According to Prelipceanu, Netverify then "extract[s] the biometric facial geometry templates of these customers and compare[s] it to their photo ID . . . so the customer can proceed to make purchases" from Jumio's Customers. *Id.* Prelipceanu further alleges that Netverify confirms consumers' ages and identities by collecting, retaining, and disclosing Biometric Data. *Id.* ¶¶ 2, 3, 19-24.

**C. The Plaintiff**

Prelipceanu is an Illinois resident who wanted to buy age-restricted products online from a Jumio Customer. To complete his purchase, he alleges that he was required to use Netverify to confirm his age. *See* Compl. ¶¶ 22, 24. Prelipceanu alleges that through the Netverify process, Jumio "took a biometric scan of [his] face through a 'face scan' taken through [his] mobile device camera." *Id.* ¶ 24. Prelipceanu does not allege where any of the circumstances relating to these events occurred, apart from a conclusory jurisdictional allegation that "the transaction out

---

because the plaintiff "invoke[d] the [defendant's] website in her complaint," the "web pages that [plaintiff] chose not to highlight [were] fair game" in the defendant's motion to dismiss).

of which this cause of action arises occurred in Cook County." *Id.* ¶ 18. He also claims, without any supporting factual allegations, that he has suffered (1) "pecuniary damages in the form of diminution in the unique identifying value of his biometrics," (2) "other costs associated with identity protection and account monitoring," and (3) "mental anguish, anxiety, and other physical injury" when he thinks about the status of his biometric information. *Id.* ¶¶ 28, 30 (diminished value and risk of exposure), ¶ 31 (anxiety).

## III. ARGUMENT

To survive a Rule 12(b)(6) motion to dismiss, a complaint must contain sufficient facts to "show[] that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). This requires a plaintiff to "provid[e] some specific facts to ground [his] legal claims," *Brooks v. Ross*, 578 F.3d 574, 581 (7th Cir. 2009), and to "give enough details about the subject-matter of the case to present a story that holds together," *Swanson v. Citibank, N.A.*, 614 F.3d 400, 404 (7th Cir. 2010). A complaint that merely alleges—but does not *show*—that the plaintiff is entitled to relief is insufficient. *See Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009). Plaintiffs cannot rely on "[t]hreadbare recitals of the elements of a cause of action," *id*. at 678, and cannot "merely parrot the statutory language of the claims that they are pleading," *Brooks*, 578 F.3d at 581. In other words, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Iqbal*, 556 U.S. at 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)).

In determining the sufficiency of a complaint under the plausibility standard, courts must "accept all well-pleaded facts as true and draw reasonable inferences in [a plaintiff's] favor." *Roberts v. City of Chi.*, 817 F.3d 561, 564 (7th Cir. 2016). A complaint that "does not give the defendants any idea of the scope of [the plaintiff's] claim or a place to begin investigating his allegations" is insufficient. *Trujillo v. Mediterranean Kitchens, Inc.*, No. 17-CV-01887, 2017 WL 2958240, at *1 (N.D. Ill. July 11, 2017).

## A. The Court Should Dismiss Prelipceanu's BIPA Claim.

### 1. Prelipceanu has not alleged facts showing the conduct at issue occurred primarily and substantially in Illinois, so he has not established that BIPA applies.

An Illinois statute cannot impose liability based on conduct occurring outside the state unless "the express provisions of the statute" make it clear that the statute is intended to apply extraterritorially. *Avery v. State Farm Mut. Auto. Ins. Co.*, 216 Ill. 2d 100, 184-85 (2005) (quoting *Dur-Ite Co. v. Indus. Comm'n*, 394 Ill. 338, 350 (1946)). "[T]here is no sign of that sort of intent from the Illinois legislature" with respect to BIPA. *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1100 (N.D. Ill. 2017); *see also* BIPA § 14/5(b) (stating that the impetus for BIPA was that the "City of Chicago and other locations *in [the] State*" had been selected to pilot new biometric-facilitated financial applications) (emphasis added). Accordingly, BIPA does not have extraterritorial effect and can impose liability based only on conduct occurring within Illinois.

Conduct is deemed to occur within Illinois when the circumstances related to a given transaction "occur[s] primarily and substantially" within Illinois. *Avery*, 216 Ill. 2d at 187; *see also Rivera*, 238 F. Supp. 3d at 1101 ("[T]here is no single formula or bright-line test for determining whether a transaction occurs within this state. Instead, a court must analyze whether the circumstances relating to the transaction occur primarily and substantially within Illinois." (internal quotation marks and citations omitted)). In the BIPA context, courts consider a variety of factors to make this determination, including, among others, (1) the plaintiff's residence, (2) the location of harm, (3) the communications between the parties (where sent and where received), (4) where a company policy is carried out, (5) where the alleged "scan of face geometry" took place, and (6) where the alleged lack of consent took place. *Rivera*, 238 F. Supp. 3d at 1101-02 (citing *Avery*, 216 Ill. 2d at 187). No single factor is determinative.

Thus, as a threshold matter, Prelipceanu must allege facts showing that the conduct at issue—Jumio's alleged collection, storage, and dissemination of Prelipceanu's Biometric Data—"occurred primarily and substantially" in Illinois. He has not done so. Instead, he has merely alleged that (1) he is an Illinois resident, (2) Jumio does business in the state of Illinois and is

registered to do so, and (3) some unidentified and unexplained "transaction" "occurred in Cook County." Compl. ¶¶ 16, 17. The first two allegations have no apparent connection to the alleged "face scan" and are therefore irrelevant to the analysis. Even if Prelipceanu is an Illinois resident, as he alleges, that says nothing about where the relevant conduct occurred. *See, e.g.*, *Walker v. S.W.I.F.T. SCRL*, 491 F. Supp. 2d 781, 795 (N.D. Ill. 2007) (holding that there was "no substantial connection to Illinois" where, as here, the complaint alleged only that "plaintiff . . . is a resident of Illinois"). Similarly, the mere fact that a defendant "does business" in Illinois (or even that the defendant is headquartered in Illinois) is insufficient to show that the *relevant conduct* occurred primarily and substantially in Illinois. *See, e.g.*, *Sheeley v. Wilson Sporting Goods Co.*, No. 17-cv-3076, 2017 WL 5517352, at *2 (N.D. Ill. Nov. 17, 2017) (dismissing claim where the "the only [alleged] link . . . [was] the fact that [the defendant was] headquartered in Illinois and that the deceptive marketing scheme at issue was created and implemented from [defendant's] headquarters").

Prelipceanu's third allegation is a mere legal conclusion. Prelipceanu cannot plausibly allege that a transaction "occurred primarily and substantially" in Illinois by nakedly asserting that it "occurred" in Cook County. *Avery*, 216 Ill. 2d at 187; *see also Iqbal*, 556 U.S.at 678 ("Threadbare recitals . . . supported by mere conclusory statements, do not suffice."). Moreover, it is unclear whether the "transaction" refers to Prelipceanu's purchase on Jumio's Customer's website, or the "face scan" that allegedly gives rise to his claim. In either case, because Prelipceanu does not provide any detail as to, for example, where the alleged scan, collection, storage, and disclosure took place, he has not alleged facts sufficient to show that BIPA applies. *Cf. Avery*, 216 Ill. 2d at 187 (relying on similar factors). This is especially true because Jumio's judicially-noticeable website makes clear that Jumio has a global customer base and is itself headquartered in California, so it would be wholly speculative to presuppose any of these Illinois contacts. *See* Ex. A. The Complaint therefore "stops short of the line between possibility and plausibility" as to the threshold issue of whether BIPA applies. *Twombly*, 550 U.S. at 557.

**2. Prelipceanu has not pled facts to support his claim that Jumio violated BIPA §§ 14/15(b) and (d).**

Subsections 14/15(b) and (d) of BIPA regulate the collection and dissemination of Biometric Data. Prelipceanu's allegations with respect to these subsections are no more than "a formulaic recitation of the elements of a cause of action," *Twombly*, 550 U.S. at 555, and "naked assertion[s]" of legal violations, *id*. at 557, that cannot withstand a motion to dismiss. *See, e.g.*, Compl. ¶¶ 21, 23. Indeed, Prelipceanu's *only* specific factual allegation about Jumio's alleged collection of his Biometric Data is that Jumio "took a biometric scan of Plaintiff's face through a 'face scan' taken through [his] mobile device camera." Compl. ¶ 24. Similarly, Prelipceanu asserts that Jumio "disseminated" and "transferred" his biometric information, without any facts to support these legal conclusions. *See id.* ¶¶ 21, 24, 46. These allegations do not state the grounds for Prelipceanu's claim that a BIPA violation occurred, much less allow Jumio to assess the "contours" of Prelipceanu's claim. *Brooks*, 578 F.3d at 581-82. Thus, Prelipceanu's allegations do not "put [Jumio] on notice of what exactly [it] might have done," *Brooks*, 578 F.3d at 582, or provide it with "a place to begin investigating his allegations," *Trujillo*, 2017 WL 2958240, at *1.

The Seventh Circuit's opinion in *Yetftich v. Navistar, Inc*. is instructive. *See* 722 F.3d 911 (7th Cir. 2013). There, the plaintiff alleged that his union acted arbitrarily in not processing his grievance but did not identify who filed the grievance, when it was filed, the content of the grievance, which union officials told him the grievance was being processed, how long he waited before concluding it was abandoned, or how he knew that that amount of time constituted "an abnormal and arbitrary delay." *Id.* at 917. Without these details, the complaint was "wholly conclusory" and did not contain sufficient "background factual content" to move the complaint "over the line from a 'possible' to a plausible claim of entitlement to relief." *Id*. Prelipceanu's allegations are equally (if not more) opaque and unsupported, and should be rejected on the same grounds. *See also Trujillo*, 2017 WL 2958240, at *1 (dismissing Fair Labor Standards Act complaint where employee alleged that he worked over 40 hours in "one or more individual work weeks" without identifying a specific week or the frequency of overtime because allegation

was insufficient to "give the defendants any idea of the scope of Trujillo's claim or a place to begin investigating his allegations"); *Hanley v. Green Tree Servicing, LLC*, 934 F. Supp. 2d 977, 983 (N.D. Ill. 2013) (dismissing Telephone Consumer Protection Act complaint where plaintiff failed to plead how many calls were made, when the calls were made, when plaintiff asked the defendant to stop making them, or how the plaintiff made the request to stop calling).

**3. Prelipceanu has not alleged facts establishing that Jumio violated BIPA § 14/15(d).**

Prelipceanu's claim for violation of subsection 14/15(d) fails for the additional reason that any alleged "disclosure" would fall squarely within BIPA's "financial transaction" exception.

Subsection 14/15(d) provides that "[n]o private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information" unless an enumerated exception applies. BIPA § 14/15(d). One such exception is subsection 14/15(d)(2), which expressly authorizes disclosure to "complete[] a financial transaction requested or authorized by the subject" of the Biometric Data. *Id.* § 14/15(d)(2).

Here, Prelipceanu alleges that Netverify "allows for both identity verification and age verification, so the customer can proceed to make purchases of both goods and services from the Defendant's clients' businesses." Compl. ¶ 2. Prelipceanu further alleges that he was only "allowed" to "proceed with his purchase" after completing the Netverify process. *Id.* ¶ 24. A "purchase" is clearly a "financial transaction" within the meaning of BIPA. *See, e.g.*, BIPA § 14/5(b) (noting that financial transactions include purchases at "grocery stores, gas stations, and school cafeterias").

In sum, BIPA expressly authorizes disclosure of Biometric Data in the circumstances alleged by Prelipceanu, and Prelipceanu has not alleged any disclosure that is not authorized by the plain language of BIPA. For both reasons, this claim is foreclosed by the plain language of BIPA.

**4. The Court should dismiss Prelipceanu's claim for violation of BIPA § 14/15(a) because Jumio has a BIPA-compliant retention policy.**

Prelipceanu also cannot state a claim under BIPA subsection 14/15(a) because his Complaint establishes that Jumio has satisfied that subsection's requirement. BIPA subsection 14/15(a) provides:

> A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

BIPA § 14/15(a).

Prelipceanu's conclusory allegation that Jumio lacks a policy that complies with this subsection is contradicted by the Jumio Privacy Policy. That policy provides in part:

> ***Facial recognition.*** If you agree to use our Netverify *with Biometric Facial Recognition*, or other facial recognition service that we offer to our customers, Jumio will collect an image of your face that you provide through a mobile app and a photo or scan of your face as it appears on an identification document. *Jumio will use facial recognition technology only for the purpose of verifying your identity as the person who appears on the identification document.* Jumio may share the facial scans with the Jumio customer through which you used Jumio's identity verification service. *Jumio will retain your facial recognition information, including the photo of your face and photo or scan of your identification document, for the amount of time requested by the Jumio customer through which you used Jumio's identity verification service. In no event will Jumio store your facial recognition information after Jumio ceases to have a customer relationship with the customer through which you used Jumio's identity verification service*.

*See* Ex. C, Jumio Privacy Policy (emphasis added); *see also* Compl. ¶ 20 & n.1 (citing webpage on which Privacy Policy link appears).

Jumio's Privacy Policy, accessible from every page on the Jumio website, is indisputably a publicly-available written policy. Its content also complies with BIPA subsection 14/15(a). BIPA does not require that private entities quote BIPA's statutory text in the policy (and no court has so held)—it requires only that they develop a retention schedule and guidelines that

substantively provide for permanent destruction of Biometric Data within the stated time frames. Jumio's Privacy Policy does this by stating that Jumio will retain facial recognition information for the amount of time requested by the Jumio Customer, but in no event after Jumio's relationship with the Customer has ended. It is the Customer, not Jumio, that has a relationship with the end user, and that is uniquely positioned to determine "when the initial purpose for collecting or obtaining such identifiers or information has been satisfied." BIPA 14/15(a). Jumio's Privacy Policy is not inconsistent with BIPA; it reflects the service provider relationship that Prelipceanu himself alleges.

In any case, and equally important, Prelipceanu has not alleged any facts plausibly suggesting that Jumio retains data longer than permitted under subsection 14/15(a). He has not alleged facts that show, for example, that the retention schedule and guidelines set forth in Jumio's policy are inconsistent with BIPA, or that Jumio's policy would result in Jumio possessing his, or anyone else's, Biometric Data for a longer period than permitted. *See* Compl. ¶ 27 (alleging that "Plaintiff is unaware of the status of his biometrics" and not that Jumio retains his biometrics). Accordingly, the Court should dismiss Prelipceanu's claim for violation of BIPA subsection 14/15(a).

**B. The Court Should Dismiss Prelipceanu's Negligence Claim.**

Prelipceanu's negligence claim must be dismissed because it improperly duplicates his BIPA claim. It is also deficient in its own right because Jumio does not owe Prelipceanu a duty of care and Prelipceanu has not alleged cognizable damage.

**1. Prelipceanu's negligence claim is duplicative of his BIPA claim.**

Prelipceanu alleges that Jumio breached a duty of care to him by "failing to implement a BIPA-compliant biometric system with reasonable data security policies," and "failing to act reasonably with respect to its biometric program." Compl. ¶¶ 57, 58. This theory is based on the same allegations that support Prelipceanu's claim that Jumio negligently failed to comply with BIPA—namely, the alleged absence of a BIPA-compliant retention policy (BIPA § 14/15(a)), the alleged absence of informed written consent for the collection of Prelipceanu's Biometric Data

(BIPA § 14/15(b)), and the alleged disclosure of Prelipceanu's Biometric Data (BIPA § 14/15(d)). In addition, the alleged damage to Prelipceanu (diminution in the value of his Biometric Data) is already alleged for the BIPA claim. *See, e.g.*, Compl. ¶ 31 (alleging damage "as a result of Defendant's conduct"). Prelipceanu's negligence claim is therefore identical to his BIPA claim and should be dismissed on that basis. *See, e.g.*, *DeGeer v. Gillis*, 707 F. Supp. 2d 784, 795-96 (N.D. Ill. 2010) (collecting cases applying the "well-settled" principle "that duplicative counts in a complaint may be properly dismissed"); *see also Neade v. Portes*, 193 Ill. 2d 433, 445 (2000) ("While pleading in the alternative is generally permitted . . . duplicate claims are not permitted in the same complaint.") (citation omitted); *cf.* Compl. ¶ 50 (pleading willful and negligent BIPA claims in the alternative).

**2. Prelipceanu has not alleged facts establishing that Jumio owed him a duty of care.**

To state a claim for negligence, a plaintiff must allege, among other things, "that the defendant owed him a duty." *Dardeen v. Kuehling*, 213 Ill. 2d 329, 336 (2004). Because Prelipceanu has not alleged facts establishing the existence of a duty, his negligence claim must be dismissed.

Illinois courts do not recognize a freestanding, common-law duty of care requiring companies to safeguard personal information, even if that personal information is sensitive. *See Cmty. Bank of Trenton v. Schnuck Mkts., Inc.*, 887 F.3d 803, 817 (7th Cir. 2018) ("Illinois has not recognized an independent common law duty to safeguard personal information."); *Dolmage v. Combined Ins. Co. of Am.*, No. 14 C 3809, 2015 WL 292947, at *6 (N.D. Ill. Jan. 21, 2015) (dismissing negligence claim based on data breach "[b]ecause there is no common law duty to protect personal information in Illinois"); *Cooney v. Chi. Pub. Sch.*, 407 Ill. App. 3d 358, 363 (2010) (negligence claim dismissed because defendant had no duty to protect against disclosure of the plaintiff's personal information, including social security numbers). Prelipceanu's mere assertion to the contrary—that Jumio "owed duties of reasonable care to Prelipceanu" because his "biometrics were obtained by [Jumio]," Compl. ¶ 56—is "entitled to no weight" and should

be disregarded. *Edgewater Beach Apartments Corp. v. Frontier Ins. Co.*, No. 08 C 5375, 2010 WL 625045, at *2 (N.D. Ill. Feb. 18, 2010).

To sidestep this problem, Prelipceanu alleges that he and Jumio were in a "special relationship." Compl. ¶ 54. But that doctrine applies only when one person owes another a duty to protect against the wrongful acts of third parties. *See Bogenberger v. Pi Kappa Alpha Corp.*, 2018 IL 120951, ¶ 33. Accordingly, the Illinois Supreme Court has recognized four "special relationships": "common carrier and passenger, innkeeper and guest, custodian and ward, and possessor of land who holds it open to the public and member of the public who enters in response to the possessor's invitation." *Id*. There is no such "special relationship" here.

Although one case in Illinois could be read to suggest that BIPA creates a duty that can be enforced through a claim for common-law negligence, Jumio respectfully submits that, to the extent the case so held, it was wrongly decided. In *Dixon v. Washington & Jane Smith Cmty.—Beverly*, the court denied a motion to dismiss plaintiff's negligence claim, finding that the plaintiff had sufficiently alleged a duty of care by alleging that the defendants had "breached their duty under BIPA to exercise reasonable care in the collection and use of her biometric data." No. 17 C 8033, 2018 WL 2445292, at *13 (N.D. Ill. May 31, 2018). But as the Seventh Circuit has explained, "only if the Illinois common law of torts imposed on [a defendant] a duty of care to [plaintiff]" can a statute then "specify the level of care that [defendant] owed [plaintiff]." *Cuyler v. United States*, 362 F.3d 949, 952 (7th Cir. 2004). Consistent with this, the cases cited in *Dixon* provide that "the violation of a statute can form the basis for a negligence action," but do not provide that statutes create a common-law duty where none previously existed. *See, e.g., Bd. of Educ. of Indian Prairie Sch. Dist. No. 204 v. Du Page Cty. Election Comm'n*, 341 Ill. App. 3d 327, 331 (2003). To the extent *Dixon* held otherwise, it went too far. In addition, the court in *Dixon* did not consider whether the plaintiff's negligence claim was duplicative of the BIPA claim.

**3. Plaintiff has not alleged facts establishing that he suffered cognizable damage proximately caused by Jumio's alleged conduct.**

Even if Prelipceanu adequately pled the existence of a duty sufficient to support his common law negligence claim, he has not alleged cognizable damage arising from any breach of that duty. "[L]egally cognizable present injury or damage" is an essential element of a negligence claim. *Yu v. Int'l Bus. Machs. Corp.*, 314 Ill. App. 3d 892, 897 (2000); *see also Shehade v. Gerson*, 148 Ill. App. 3d 1026, 1031 (1986) (affirming dismissal of negligence claim for failure to plead recoverable damages). An injury "must be actual; the threat of future harm not yet realized is not enough." *Fox v. Cohen*, 84 Ill. App. 3d 744, 751 (1980). Only damages that are proximately caused by the defendant are cognizable under a negligence claim. *See Kohn v. Laidlaw Transit, Inc.*, 347 Ill. App. 3d 746, 757 (2004). Prelipceanu alleges that he suffered damages in the form of: (1) "pecuniary damages in the form of diminution in the unique identifying value of his biometrics," (2) "other costs associated with identity protection and account monitoring," and (3) "mental anguish, anxiety, and other physical injury" when he thinks about the status of his biometric information. Compl. ¶¶ 28, 30 (diminished value and risk of exposure), ¶ 31 (anxiety). None of these purported harms suffice.

***Diminution in value of biometrics.*** The only form of damage Prelipceanu specifically identifies in the negligence count is the alleged diminution in the value of his biometrics. *See* Compl. ¶ 58. But that alleged damage is only conclusorily alleged and so cannot support a claim for negligence. For example, Prelipceanu does not plead facts explaining why his biometric information is economically valuable, what value it had prior to Jumio's alleged collection, what value the information had after, or how Jumio's alleged collection proximately caused the value to decrease. *See, e.g.*, *Camasta v. Jos. A. Bank Clothiers, Inc.*, 761 F.3d 732, 739-40 (7th Cir. 2014) (allegation that plaintiff paid more than the value of merchandise he received was conclusory and insufficient to establish actual damages).

***Costs associated with identity protection and account monitoring.*** Even if Prelipceanu asserts that Jumio's negligence caused him to incur costs associated with identity protection, that harm is also not cognizable because it is based entirely on the hypothetical risk of future identity

theft. *See* Compl. ¶ 30 ("Plaintiff faces additional risks if Defendant were to suffer a data breach."). Fear of a future harm is not cognizable damage. *See Fox*, 84 Ill. App. 3d at 751; *see also Henderson v. Blatt*, No. 14 C 7517, 2015 WL 2399124, at *3 (N.D. Ill. May 14, 2015) ("Allegations premised on the belief of injury not factually pleaded must be read out of the complaint as conclusory."). And costs incurred due to that speculative fear are not proximately caused by Jumio's alleged violation of the statute. *See Kalata v. Anheuser-Bush Co.*, 144 Ill. 2d 425, 437 (1991) ("Liability may not be based upon speculation, imagination, or mere conjecture."); *Worix v. MedAssets, Inc.*, 857 F. Supp. 2d 699, 705 (N.D. Ill. 2012) (dismissing negligence claim based on alleged data breach because "an increased risk of identity theft, even accompanied by credit-monitoring costs, does not constitute present injury under Illinois law"); *Walker v. Macy's Merch. Grp., Inc.*, 288 F. Supp. 3d 840, 856 (N.D. Ill. 2017) ("Proximate cause is not established, however, where the causal connection is contingent, speculative or merely possible." (quoting *Mengelson v. Ingalls Health Ventures*, 323 Ill. App. 3d 69, 75 (2001)).

***Mental anguish, anxiety, and other physical injury.*** Finally, Prelipceanu's allegation that he suffers from "mental anguish, anxiety, and other physical injury," Compl. ¶ 31, is not cognizable damage. Illinois' "impact rule" does not allow a plaintiff to recover damages for emotional distress unless the complaint alleges contemporaneous physical injury or impact. *Schweihs v. Chase Home Fin., LLC*, 2016 IL 120041, ¶ 38; *Hart v. Amazon.com, Inc.*, 191 F. Supp. 3d 809, 821 (N.D. Ill. 2016), *aff'd*, 845 F.3d 802 (7th Cir. 2017). Here, Prelipceanu's allegation of "other physical injury" is conclusory and implausible—not a single fact alleged in the Complaint supports the bare assertion that he suffered actual physical injury due to his thoughts about his Biometric Data. *Cf. Glob. Cash Network, Inc. v. Worldpay, US, Inc.*, 148 F. Supp. 3d 716, 723 (N.D. Ill. 2015) (allegation that plaintiff suffered "other nonmonetary injury" was a "purely conclusory assertion" that should not be credited). Prelipceanu cannot avoid Illinois' impact rule by conclusorily alleging physical injury. *See Hart*, 191 F. Supp. 3d at 821 (holding that the plaintiff could not recover for alleged emotional distress when the complaint

"included no allegations to plausibly suggest 'a contemporaneous physical injury or impact' due to [the defendant]'s alleged negligence") (citation omitted).

## IV. CONCLUSION

For the reasons set forth above, Jumio respectfully submits that this Court should dismiss the Complaint pursuant to Federal Rule of Civil Procedure 12(b)(6).

Dated: March 29, 2019

Respectfully Submitted,

**JUMIO CORPORATION**

By: */s/* Susan D. Fahringer
Susan D. Fahringer
One of its Attorneys

Susan D. Fahringer
SFahringer@perkinscoie.com
PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101-3099
Telephone: (206) 359-8000
Facsimile: (206) 359-9000
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

Debra R. Bernard, Bar No. 39225
DBernard@perkinscoie.com
PERKINS COIE LLP
131 S. Dearborn Street, Suite 1700
Chicago, IL 60603
Telephone: (312) 324-8400
Facsimile: (312) 324-9400

Nicola C. Menaldo (*Pro Hac Vice*)
NMenaldo@perkinscoie.com
PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101-3099
Telephone: (206) 359-8000
Facsimile: (206) 359-9000
*PRO HAC VICE*
*ATTORNEY TO BE NOTICED*

**CERTIFICATE OF SERVICE**

I hereby certify that, on March 29, 2019, a copy of the foregoing JUMIO CORPORATION'S MEMORANDUM OF LAW IN SUPPORT OF ITS MOTION TO DISMISS PLAINTIFF'S COMPLAINT was served via the Court's ECF filing system to the following attorneys of record:

Myles McGuire
David L. Gerbie
Jad Shekali
MCGUIRE LAW, P.C. (Firm ID: 56618)
55 W. Wacker Drive, 9th Fl.
Chicago, IL 60601
Telephone: (312) 893-7002
Facsimile: (312) 275-7895
mmcguire@mcgpc.com
dgerbie@mcgpc.com
jsheikali@mcgpc.com

/s/ Susan D. Fahringer

# EXHIBIT A

Request Sales Information



# About Jumio

# About Jumio

## When identity matters, trust Jumio.

Thanks to data breaches, cybercriminals, and compliance mandates, it's never been harder or more important to establish trust online.

As traditional methods of verification, including simple passwords, knowledge-based authentication, and SMS passcodes have proven vulnerable, governments, regulators, and enterprises are being forced to find more robust, secure, and reliable verification methods to definitively establish identity.

**Connecting a person's online and real-world identities is the sweet spot of Jumio.**

Whether in front of a webcam or a smartphone, we can quickly verify the authenticity of an ID, a document, or your user's real-world identity in seconds—not hours or days—helping you optimize conversions, deter fraud, and meet compliance mandates while providing a fast, seamless customer experience.

Jumio uses computer vision technology, machine learning and live verification experts to verify credentials (e.g., passports, drivers licenses, etc.) issued by over 200 countries. Our technology powers businesses with scalable, secure and compliant identity verification, which enables them to build and sustain trust in an increasingly unsafe digital world.

Jumio is widely considered to be the largest and most accurate solution in the market and used by leading companies in the financial services, sharing economy, retail, travel, blockchain and online gaming sectors.

Based in Palo Alto, California, and funded by Centana Growth Partners and Millennium Technology Value Partners, Jumio operates globally, with offices in the US, Europe, and Asia Pacific and has been the recipient of numerous awards for innovation, including this year's Frost & Sullivan's North American Entrepreneurial Company of the Year for the Biometric Security Solutions Industry.

# Locations

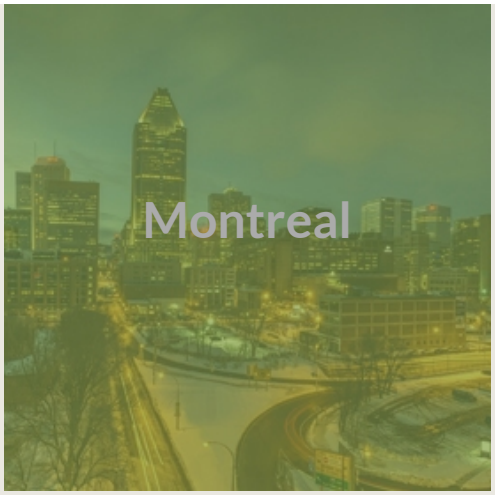

Palo Alto,
California


London,
United Kingdom


Vienna,
Austria


New York,
New York


Singapore


Montreal


Rajasthan,
India


Linz,
Austria


Barranquilla,
Colombia

© 2010 – 2019 Jumio | All rights reserved. | US Patent App. | Privacy Policy | Contact | Partner Program | Partner Resources | Netverify Login

# EXHIBIT B

Request Sales Information

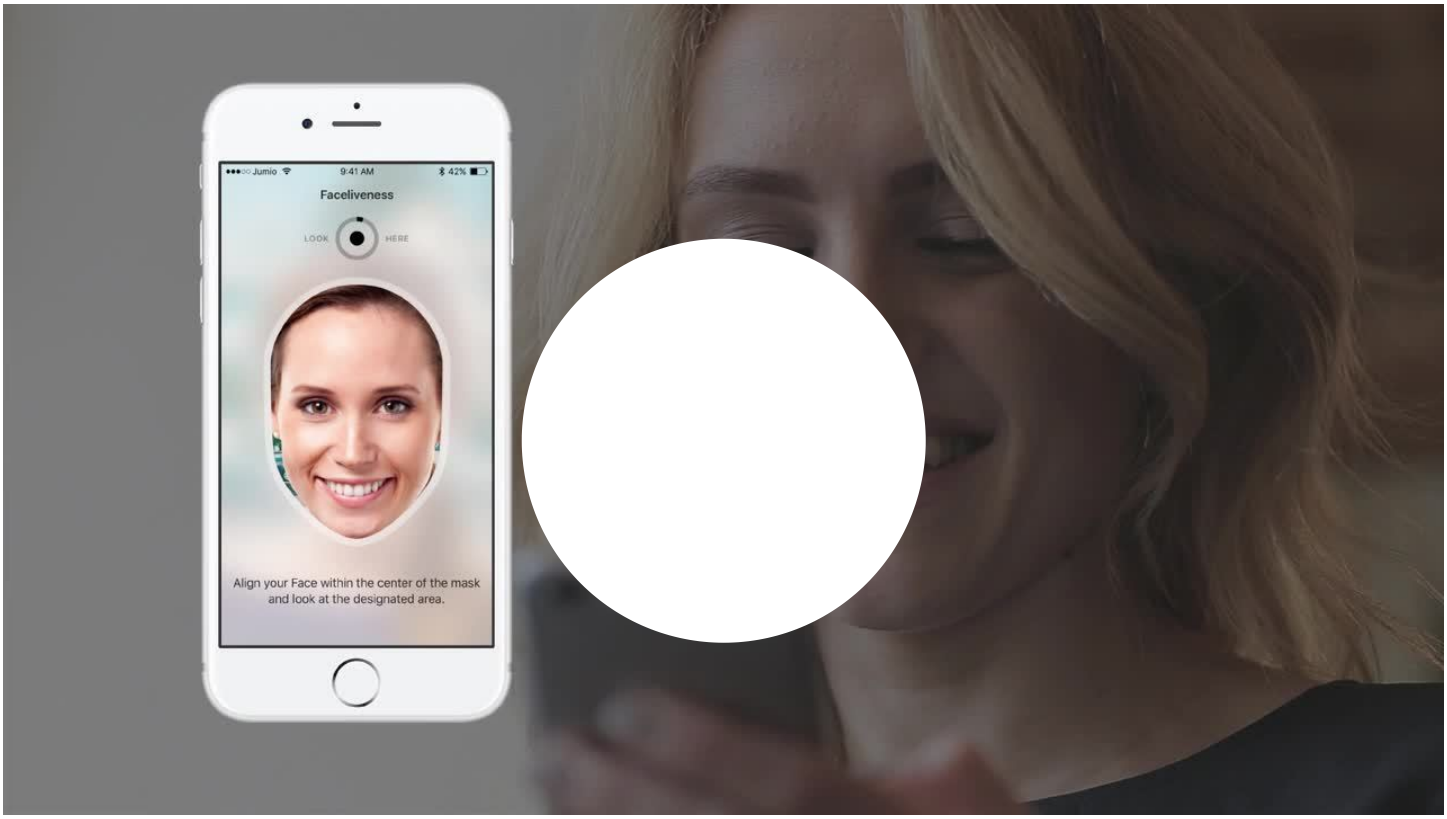
Home Solutions Features Use Cases Industries About Resources Contact

Trusted Identity as a Service

# End-to-End AI-Powered Identity Verification & Authentication

With identity theft and account takeover on the rise, it's increasingly difficult for businesses to trust that someone is who they claim to be online. Jumio's identity verification and authentication solutions leverage the power of

biometrics, AI and the latest technologies to quickly verify the digital identities of new customers and existing users.




Watch the 2-Minute Explanation

## Jumio ID Verification

Determine if an ID is authentic and belongs to the user.

## Jumio Identity Verification

Ensure that the person behind a transaction is who they say they are.

## Jumio Document Verification

Perform online address verification with ease.

## Jumio Authentication

Replace outdated KBA and 2FA with the simplicity and security of a selfie.

# Trusted Identity as a Service Benefits

### Optimize Conversions

Jumio provides an intuitive and satisfying user experience that takes less than a minute to complete.

### Cross-Platform Support

Jumio seamlessly integrates into websites, iOS or Android applications via APIs, SDKs and webcams.

### Secure Data Storage

All data is transmitted and stored with strong AES 256 bit encryption. Jumio is PCI Level 1 compliant.

### Global Footprint

Jumio supports more countries, languages, and document types than any other solution.

### Fast Implementation

Quickly integrates into your website or mobile app and business processes.

### The UX Experts

We'll share the magic and best practices for how to introduce your users to online verification and how to minimize the friction associated with robust identity verification.

**Download the Product Datasheet >**

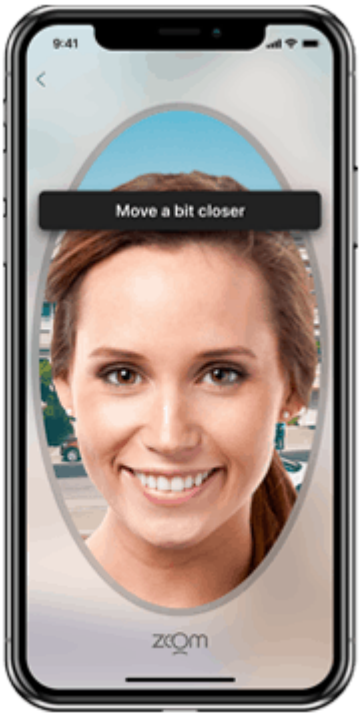
## Featuring


## Jumio ID Verification

Detect more fraud by scanning a user's government-issued ID to ensure that it has not been digitally manipulated.

- Ensure error-proof image capture.
- Deliver an effortless customer experience.
- Increase completion rates for business transactions and account openings.
- Catch fake IDs and prevent fraud.

**Learn More**




## Jumio Identity Verification

Determine if the person behind a transaction is present and who they say are.

- Ensure customer presence with FaceTec ZoOm® Certified 3D Liveness Detection.
- Compare photo ID to real world “selfie” to ensure against identity theft and deter fraudsters.
- Deliver a definitive yes or no decision in seconds.
- Dramatically reduce user friction and verification time with award-winning UX best practices.

Learn More



## Jumio Document Verification

Provide online address verification by scanning and extracting data from utility bills, credit card and bank statements even if they're creased or crumpled.

- Meet KYC compliance and EU AML directives.
- Securely and easily establish proof of residence.

- Scan utility bills, bank statements, and more.
- Extract and return pertinent customer data.

Learn More

---


## Jumio Authentication

Leverage face-based biometrics to deliver a significantly more reliable authentication experience than passwords, out-of-band authentication and KBA.

- Leverage face-based biometrics to deliver a significantly more reliable authentication experience than passwords, 2FA and KBA.
- Provide an intuitive, user-friendly experience on all channels without compromising security.

- Deter would-be fraudsters and protect against sophisticated spoofing attempts.

Learn More


## Get Started

Let a Jumio expert show you how easy it can be to integrate our suite of verification solutions to your website or mobile experience. Start by requesting more information and we'll be in touch shortly.

Request More Information

© 2010 – 2019 Jumio | All rights reserved. | US Patent App. | Privacy Policy | Contact | Partner Program | Partner Resources | Netverify Login

# EXHIBIT C

Request Sales Information

Home Solutions Features Use Cases Industries About Resources Contact

# Jumio Corp. Privacy Policy for Online Services

Jumio Corporation ("Jumio") respects the privacy of our users. This Privacy Policy ("Policy") describes our privacy practices concerning information collected in connection with Jumio's payment, verification, and related online services, including Fastfill, Netswipe, and Netverify (the "Services"). A separate policy, available here, describes our privacy practices in connection with our online website, located at www.jumio.com.Jumio makes the Services available to third parties for integration into those third parties' websites, applications, and online services. Jumio collects, uses, and discloses individual users' information *only* as directed by these third parties and, accordingly, Jumio is a mere processor of user information with respect to the Services and not a controller. Further, some features of the Services may be disabled or altered by the data controller, or the controller may require Jumio to collect, use, disclose, or otherwise process data in ways that differ from those described below. Thus, to fully understand how your information will be handled when you use the Services, you must review not just this Policy, but also the privacy policy of the third party with whom you are dealing directly (the "Third-Party Data Controller").

Notwithstanding the above, Jumio may process certain individual users' information in anonymized form for its own purposes.

Jumio is headquartered in the United States at 268 Lambert Avenue, Palo Alto, CA 94306.

## What personal and other information Jumio collects about you

Jumio collects "personal information" about users of the Services. "Personal information" is information such as a name, email address, or identification card image, which refers to an identified or identifiable person. Jumio processes personal information on behalf of the Third-Party Data Controller. For its own purposes, Jumio processes only anonymized information. "Anonymized information" is information which does not relate to an identified or identifiable person or is rendered anonymous in such a manner that the person is no longer identifiable.

***Personal information.*** Jumio collects a wide range of personal information through the Services. This information varies depending on the Jumio application and the Third-Party Data Controller in question, but may include such information as name, physical address, email address, telephone number, social security number, driver's license number, state or national ID card number, passport number, other ID card number, credit or debit card number, CVV, expiration date, and/or date of birth. In some cases, Jumio may collect a visually scanned or photographed image of your face and/or your identification card, driver's license, passport, utility bill, bank account statement, insurance card, or credit/debit card. This image may include your photograph and other information from the imaged document, such as your eye colour, weight, height, and organ donor status.

***Facial recognition.*** If you agree to use our Netverify with Biometric Facial Recognition, or other facial recognition service that we offer to our customers, Jumio will collect an image of your face that you provide through a mobile app and a photo or scan of your face as it appears on an identification document. Jumio will use facial recognition technology only for the purpose of verifying your identity as the person who appears on the identification document. Jumio may share the facial scans with the Jumio customer through which you used Jumio's identity verification service. Jumio will retain your facial recognition information, including the photo of

your face and photo or scan of your identification document, for the amount of time requested by the Jumio customer through which you used Jumio's identity verification service. In no event will Jumio store your facial recognition information after Jumio ceases to have a customer relationship with the customer through which you used Jumio's identity verification service.

***Data provided by third parties.*** We may receive personal or anonymized information about you from the Third-Party Data Controller that integrates the Services into its website, application, or other online service. This information includes a customer ID, selected by the Third-Party Data Controller, that uniquely identifies you in the third party's database. For additional information, review the privacy policy of the Third-Party Data Controller.

At the direction of the Third-Party Data Controller, Jumio also might obtain information about you from other third parties, such as consumer reporting agencies and fraud-prevention services.

***Cookies and other tracking data.*** When you use the Services, we automatically receive and record certain information from your computer (or other device) and/or your web browser. This may include such information as the third-party website or application into which the Services are integrated, the date and time that you use the Services, your IP address and domain name, your software and hardware attributes (including operating system, device model, and hashed device fingerprint information), and your general geographic location (*e.g.*, your city, state, or metropolitan region). We will process such data only as instructed by the Third-Party Data Controller.

We also use cookies in connection with the Services. For further information please refer to the section entitled "Cookies" below.

# Cookies

***What are cookies?*** Cookies are small files that are stored on your computer or other device by your web browser. A cookie allows Jumio to recognize whether you have used the Services before and may store user preferences and other information.

***How are cookies used?*** For example, cookies can be used to collect information about your use of the Services during your current session and over time, your computer or other device's operating system and browser type, your Internet service provider, your domain name and IP address, and your general geographic location. We process personal information generated by cookies only as instructed by the Third-Party Data Controller.

***What kind of cookies are used on the Website?*** Our website primarily uses the following types of cookies:

| Cookie Name | Cookie Type | Purpose |
|---|---|---|
| __ga | Persistent cookie | This cookie is used to distinguish users and expires after 2 years. |
| __gat | Session cookie | This cookie is used to throttle the request rate and expires after 10 minutes. |

"Session cookies" are temporary bits of information which are deleted when you exit your web browser. Session cookies are typically used to improve navigation and to collect web statistics.

"Persistent cookies" are more permanent bits of information that are stored and remain on your computer until they are deleted by you. This type of cookie stores information on your computer for a number of purposes; such as saving your passwords. Persistent cookies delete themselves after a certain period of time but are renewed each time you visit the website.

***How do you avoid cookies?*** If you are concerned about having cookies on your computer or device, you can set your browser to refuse all cookies or to indicate when a cookie is being set, allowing you to decide whether to accept it. You can also delete cookies from your computer. However, if you choose to block or delete cookies, certain features of the Services may not operate correctly.

## How Jumio uses the personal and anonymized information that we collect

In general, Jumio uses the personal and anonymized information that we collect in connection with the Services as discussed in this section of the Policy.

Personal information is used by Jumio *only* as directed by the Third-Party Data Controller that integrates the Services into its website, application, or other online service. Subject to the privacy policy of the Third-Party Data Controller, we use your personal information as follows on behalf of the Third-Party Data Controller:

Jumio may use your personal information to provide the Services. For example, we might use your credit card information or ID card information to populate an online form, or to verify your identity in connection with your use of another online service. We also may use your personal information to fulfill the terms of any agreement between us and the Third-Party Data Controller; to complete a transaction that you initiate; to deliver confirmations, account information, notifications, and similar operational communications; and to comply with legal and/or regulatory requirements.

Anonymized information that we collect in connection with the Services is used by Jumio for its own purposes to perform analytics and research concerning the Services.

## How Jumio shares personal and anonymized information with third parties

In general, Jumio shares the personal and anonymized information that we collect in connection with the Services as discussed below.

However, Jumio shares personal information *only* as directed by the Third-Party Data Controller, and thus the following language is subject to the privacy policy of the Third-Party Data Controller.

***Third-Party Data Controller.*** We share the personal and pseudonymized information that we collect on behalf of a particular Third-Party Data Controller with that Third-Party Data Controller.

***Jumio service providers.*** Jumio also uses third-party service providers to help us deliver, manage, and improve the Services. These service providers may collect

and/or use your personal information or anonymized information to assist us in achieving the purposes discussed above in the section entitled "How we use the personal and non-personal information that we collect." For example, we use a third party to help us translate the information contained in scanned images of identification cards.

We also may share your personal information with other third parties when necessary to fulfill your requests for services; to complete a transaction that you initiate; or to meet the terms of any agreement that you have with us or our partners.

***Analytics providers.*** We partner with certain other third parties to collect anonymized information and engage in analysis, auditing, research, and reporting.

***Legal purposes.*** We also may use or share your personal information with third parties when we have reason to believe that doing so is necessary:

- to comply with applicable law or a court order, subpoena, or other legal process;
- to investigate, prevent, or take action regarding illegal activities, suspected fraud, violations of our terms and conditions, or situations involving threats to our property or the property or physical safety of any person or third party;
- to establish, protect, or exercise our legal rights or defend against legal claims; or
- to facilitate the financing, securitization, insuring, sale, assignment, bankruptcy, or other disposal of all or part of our business or assets.

***Aggregated information.*** From time to time, Jumio may also share anonymized and aggregated information about users of the Services, such as by publishing a report on trends in the usage of the Services.

## Security

Jumio uses commercially reasonable physical, electronic, and procedural safeguards to protect your personal information against loss or unauthorized access, use, modification, or deletion. Among other things, Jumio encrypts sensitive information both in transit and at rest. Jumio is PCI Level 1 compliant and regularly conducts

security audits, vulnerability scans, and penetration tests to ensure compliance with security best practices and standards. However, no security program is foolproof, and thus we cannot guarantee the absolute security of your personal or other information. Moreover, we cannot guarantee the safety of your information when in the possession of other parties, such as the Third-Party Data Controller.

## Reviewing and updating your information

Jumio will grant you access to your personal information as directed by the Third-Party Data Controller that integrates the Services into its website, application, or online service. Jumio also will retain your personal information as directed by the Third-Party Data Controller and, accordingly, we may retain your personal information for as short as a few minutes or as long as five years.

Thus, if you want to learn more about the personal information that Jumio has about you, or you would like to submit a request to update or change that information, please contact the Third-Party Data Controller. You also may reach us by email at privacy@jumio.com.

## Information for users of the Services from outside the United States

The personal information that Jumio collects through or in connection with the Services is transferred to and processed in the United States for the purposes described above. Jumio also may subcontract the processing of your data to, or otherwise share your data with, affiliates or third parties in the United States or countries other than your country of residence. The data protection laws in these countries may be different from, and less stringent than, those in your country of residence.

However, we only transfer your personal data to countries where the EU Commission has decided that they have an adequate level of data protection or we take measures to ensure that all recipients provide an adequate level of data protection. We do this for example by entering into appropriate data transfer

agreements based on Standard Contractual Clauses (2010/87/EC and/or 2004/915/EC).

## Children's Privacy

The Services are not directed to children under the age of 13, and Jumio will never knowingly collect personal or other information from anyone it knows is under the age of 13. We recommend that persons over 13 but under 18 years of age ask their parents for permission before using the Services or sending any information about themselves to anyone over the Internet.

## Changes to this Policy

Technology and the Internet are rapidly changing. Jumio therefore is likely to make changes to the Services in the future and as a consequence will need to revise this Policy to reflect those changes. When we revise the Policy, Jumio will post the new Policy on the Jumio website's home page (www.jumio.com), so you should review that page periodically. If we make a material change to the Policy, you will be provided with appropriate notice. If we maintain your email address, we also may email you a copy of the revised Policy at your most recently provided email address. It is therefore important that you update your email address if it changes.

## Questions or comments

If you have any questions or comments regarding our Policy, please mail or email us at:

Jumio Corporation

268 Lambert Avenue

Palo Alto, CA 94306

Email: privacy@jumio.com

***Effective date:*** March 27, 2018

© 2010 – 2019 Jumio | All rights reserved. | US Patent App. | Privacy Policy | Contact | Partner Program | Partner Resources | Netverify Login